UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,986	09/29/2006	Neville Robert Jones	8235.008.PCUS00	3283

26474 7590 12/23/2009

NOVAK DRUCE DELUCA + QUIGG LLP
1300 EYE STREET NW
SUITE 1000 WEST TOWER
WASHINGTON, DC 20005

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/594,986	JONES ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,14-16,18-30,33-45 and 67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12, 14-16, 18-30, 33-45, and 67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on September 11, 2009. Claims 1-45 were previously pending consideration. Per the received amendment, claims 11, 13, 17, 31, 31 and 46-66 are cancelled, and claims 67 is added.

2. Claims 1-10, 12, 14-16, 18-30, 33-45, and 67 are currently pending consideration.

Response to Arguments

Applicant's arguments filed September 11, 2009 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Bandini (U.S. Patent Pub. No. 2008/0270789) in view of Elliot (U.S. Patent 6,335,927), does not disclose receiving a request for key request and authentication credentials and based on the authentication credentials providing the key container. The Applicant seems to focus on the use of the authentication credentials when arguing that the combination of Bandini and Elliot fails to teach the disclosed limitation. However, the use or motivation of combination is not dispositive. Elliot discloses an authentication server which authenticates a user by checking a user name and password (authentication credentials) (column 256, lines 10-32). Once this user is authenticated, then the certificate look up would be verified in Bandini and the key container would be provided

(Bandini: paragraph 66). Therefore, based on who the user is (user name and password) a particular key container is provided (determined type) to the user (Bandini: paragraph 66). Therefore, the argument is not found persuasive.

Furthermore, the Applicant argues that the CPA does not teach an address of a sender being transmitted, as it discloses just a key pair and a public key certificate. However, it is well-known in the art that the certificate is used to bind a public key to an individual by their address (IP address). Therefore, the fact that a public key certificate is sent, mans that an address of the sender or recipient is also sent. Therefore, the argument is not found persuasive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10, 12, 14-16, 18-30, 33-45, and 67 are rejected under 35 U.S.C. 103(a) as being obvious over Bandini et al. (US 2008/0270789) in view of Elliott et al. (US 6,335,927).

Regarding Claims 1, 9-10, 30, 33:

Bandini discloses a method of providing a key container ("Digital Certificates" See paragraphs 41 and 44) by a key container directory ("Certificate Lookup Server" See fig. 12 ref. no. 1210 and paragraphs 58-59), the key container to be used to secure a message that will be sent from a sender to a recipient ("Encryption/signature and/or decryption/verification of messages between transmitting and receiving cites" See figs. 5(a)-5(c) and paragraphs 43-46), receiving a request for the key container from a requestor ("The e-mail firewall submits the e-mail address of the recipient or the domain of the recipient's e-mail to the certificate lookup and verification server and optionally submitting a description of the policy requirements, or preferences, for the certificates." See paragraph 65 and "Client 508.1 provides encryption/decryption services to allow messages to be transmitted securely through server 506 by supporting encryption/decryption services." See paragraph 45), and in response to the request providing a key container to the requestor that contains a cryptographic key of a gateway that the message will transmit ("The response, which includes a sorted list of one or more certificates is returned by the certificate lookup and verification server to the security manager of the e-mail firewall." See paragraph 65) and an address of the sender or the recipient ("Identification of the other S/MIME server through directory domain records, association of directory domain records with server certificates and selection of encryption/signature algorithms and key length." See paragraph 44 and "Identification of the client 508.1 through directory user records with user certificates and selection of encryption/signature algorithms and key length." See paragraph 45).

Bandini discloses the above stated method for messaging security having the communication between the e-mail firewall and the certificate lookup and verification server authenticated (See paragraph 66).

Bandini does not disclose the authentication is through the use of a valid username and password combination.

Elliot discloses an authentication server that authenticates a user by checking a user name and password against a database of valid user names and passwords (See col. 256 lines 10-32).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Bandini to include checking a user name and password against a database of valid user names and passwords such as that taught by Elliott in order to prevent unauthorized users from accessing the certificate lookup and verification server.

Regarding Claims 2-3 and 44:

Bandini discloses the key container directory is remote from the gateway and external to the network domain of the recipient ("An external certificate lookup server 1210 is employed to provide security data, including certificate date to e-mail firewalls." See fig. 12 ref. no. 1210 and paragraph 58).

Regarding Claim 4:

Bandini discloses the message is transmitted from the sender over an insecure computer network ("Internet" See fig. 5(a)-5(c) ref. no. 104).

Regarding Claim 5:

Bandini discloses the network domain of the recipient is secure ("A first plurality of user computers 1208 is coupled to a first firewall 1202 by a local connection. In one embodiment the local network connection between the user computers 1208 and the e-mail firewall 1202 is a secure private network, as is known in the art." See fig. 12 ref. nos. 1202, 1208, and paragraph 58).

Regarding Claim 6:

Bandini discloses providing a key container having a key container for each gateway that the message will transit ("The response, which includes a sorted list of one or more certificates is returned by the certificate lookup and verification server to the security manager of the e-mail firewall." See paragraph 65).

Regarding Claim 7:

Bandini discloses determining the identity of one or more gateways that the message will transit ("Identification of the other S/MIME server through directory domain records, association of directory domain records with server certificates and selection of encryption/signature algorithms and key length." See paragraph 44).

Regarding Claim 8:

Bandini discloses the key container directory provides multiple key containers in the response to the request ("The response, which includes a sorted list of one or more certificates is returned by the certificate lookup and verification server to the security manager of the e-mail firewall." See paragraph 65).

Regarding Claims 12:

Bandini discloses determining whether the requestor is the sender of the message and if so providing an encryption key container to the requestor ("The security manager 226 is accessing the recipient's or the e-mail firewall's public key." See paragraph 56).

Regarding Claim 14:

Bandini discloses determining whether the requestor is from the same domain as the gateway and if so, Providing the encryption key container having the cryptographic key of the requestor's gateway ("A message by client 508.2 to client 508.1 may be encrypted when transmitted to server 105.1, decrypted by server 105.1 and subjected to appropriate actions by the policy managers. The message may then be encrypted for transmission to server 105.2 decrypted by server 105.2 and Subjected to appropriate actions by the policy managers, and encrypted for transmission to client 508.1 which decrypts the message." See fig. 5(c) and paragraph 46).

Regarding Claim 15:

Bandini discloses the requestor is the gateway and the request includes the address of the sender ("The e-mail firewall submits the e-mail address of the recipient or the domain of the recipient's e-mail." See paragraph 65).

Regarding Claims 16 and 38-40:

Bandini discloses the requesting the key contain includes an indication that a signing key container is requested ("The S/MIME protocol is well known and widely used and provides encryption and digital signatures." See paragraph 41).

Regarding Claims 18-20:

Bandini discloses the e-mail firewall determines if the e-mail message is such that a signature is added and an e-mail firewall policy refers to the e-mail message textual content, destination, source, and size, in determining whether a signature is required (See paragraph 55)

Regarding Claim 21:

Bandini discloses the requestor authenticating with the key container directory ("The communication between the e-mail firewall and the certificate lookup and verification server is preferably authentication." See paragraph 66).

Regarding claims 22-23,

Bandini discloses the above stated method for messaging security having the communication between the e-mail firewall and the certificate lookup and verification server authenticated (See paragraph 66).

Bandini does not disclose the authentication is through the use of a valid username and password combination.

Elliot discloses an authentication server that authenticates a user by checking a user name and password against a database of valid user names and passwords (See col. 256 lines 10-32).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Bandini to include checking a user name and password against a database of valid user names and passwords such as that taught by Elliott in order to prevent unauthorized users from accessing the certificate lookup and verification server.

Regarding Claim 24:

Bandini discloses once the request has been received generating the request key container ("The e-mail firewall submits the e-mail address of the recipient or the domain of the recipient's e-mail to the certificate lookup and verification server and optionally submitting a description of the policy requirements, or preferences, for the certificates. The certificate lookup and verification server responds by facilitating the lookup and verification according to its own policies or according to the policies submitted by the e-mail firewall." See paragraph 65).

Regarding Claim 25:

Bandini discloses the request is made using a Lightweight Directory Access Protocol ("The certificate lookup module preferably employs the Light-weight Directory Access Protocol to query the remote servers for certificates." See paragraph 61).

Regarding Claim 26:

Bandini discloses the key container contains a cryptographic key that is a public key ("E-mail firewalls provide key pair and public key certificate generation." See paragraph 44).

Regarding Claim 27:

Bandini discloses the key container is a digital certificate ("S/MIME advantageously offers security services for authentication using digital certificates." See paragraph 41).

Regarding Claim 28:

Bandini discloses the key container is a Pretty Good Privacy public key ("It should be understood that other secure message protocols such as Pretty Good Privacy or Open PGP, as specified y the ITF working group may also be used.").

Regarding Claim 29:

Bandini discloses the address contained in the key container is an e-mail address ("An e-mail from a company's CEO to the company's legal counsel by the domain of full –email address can be specified to require either encryption, signature, or both." See paragraph 39) and the gateway is an e-mail gateway ("Mail Server" See figs. 5(a)-5(c) and "E-mail Firewall" See fig. 12 ref. nos. 1202 and 1203).

Regarding Claims 34-36 and 42:

Bandini discloses encryption is preferably performed by one of the following symmetric encryption algorithms: DES, Triple-DES, RC2, and other algorithms introduced by revisions of the S/MIME standard (See paragraph 41).

Regarding Claim 37:

Bandini discloses the sender's address is from the same domain as the gateway ("A first plurality of user computers 1208 is coupled to a first firewall 1202 by a local connection. In one embodiment the local network connection between the user computers 1208 and the e-mail firewall 1202 is a secure private network, as is known in the art." See fig. 12 ref. nos. 1202, 1208, and paragraph 58).

Regarding Claim 41:

Bandini discloses the key container includes information that permits a requestor to determine the authenticity and integrity of the key container ("When the source of

digital certificates is not fully trusted, the security manager 226 first verifies the validity of the digital certificate before employing it to encrypt a message." See paragraph 56)

Regarding Claim 43:

Bandini discloses the key container includes information about the key container directory that provided the key container ("The policy actions include verifying the signing certificate against a configurable list, verifying the digital certificate validity dates, verifying the key strength and algorithm allowed by the certificate, verifying the certificate usage, verifying the certificate chain, verifying that the root certificate is in a list of acceptable root certificate, and verifying that the certificate is not revoked." See paragraph 50).

Regarding Claim 45:

Bandini discloses the key container directory has a datastore of cryptographic keys that can be contained in any provided key container ("The certificate lookup server 1210 preferably stores security data that is available to security processes in the firewalls 1202, 1203 for facilitating secure communications of e-mail messages over the public network 1204.").

Regarding claim 67,

Bandini discloses a key container wherein the step of determining comprises in the event the requestor is anonymous, the determined type of container is an encryption key container (a key pair and a public key certificate, wherein the certificate is used to bind a public key to an individual by their IP address" (paragraph 45, and 65).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
12/09/2009
Primary Examiner, Art Unit 2431